Appendix M. EC Security Management

INTRODUCTION

The Federal government has emphasized the rapid expansion of electronic data interchange (EDI) as an accepted business technology for participating in today's global market. EDI holds great promise for improving the quality and efficiency of Federal procurement. However, this technology will not be implemented in a risk free environment. Government agencies must ensure that full consideration is given to the risk issues inherent in the use of computers and telecommunications to accomplish traditional paper-based administrative functions. Without an appropriate level of security and control, EC operation will be unreliable, and losses will be unnecessarily high. While EC systems must be protected against fraud and unauthorized disclosure of information, protection against accidents, errors, and omissions is equally important. Due to the increased processing speed of EC transactions, the cost to recover from the consequences of errors and omissions tends to be greater than with traditional business systems. Prompt, accurate, and automated detection of errors and omissions is an important requirement of EC systems.

LEGAL REQUIREMENTS

Issues of legal admissibility and computer security are intertwined and must be considered together. Questions of legal validity/admissibility and computer security are but two sides of the same coin. Systems managers should retain the services of a computer security specialist during the design of an EDI application so that the requirements of the Computer Security Act will be satisfied. By the same token, the systems manager should also retain a competent litigator during this design process to maximize the likelihood that the outputs of the application will be admissible as evidence. Recognition of this essential unity between system integrity and the evidentiary value of system outputs should help to alleviate unfounded, but often expressed, concerns regarding whether electronic documents and their various signature analogues are “legal.” Indeed, these concerns should by now have definitively been laid to rest. In general, signature and writing requirements are not legal barriers to electronic commerce.

The Computer Security Act of 1987 provides a framework for determining what security characteristics are appropriate for particular applications. The Act defines sensitive information as including "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy [of] individuals. ..." It requires each agency to consider the risk to such sensitive information and to "establish a plan for the security and privacy of each Federal computer system ... that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse or unauthorized access to or modification of the information contained in such system." Hence the organization must develop security plans and perform risk analysis for their application systems.

In the realm of security, "one size" does not fit all, just as in the law of evidence the foundational showing will vary with the particular circumstances. A simple hypothetical case should make the point. Party A sends Party B an electronic purchase order in a standard EDI format. Parties Y and Z do the same. In both cases, disputes arise necessitating the use of the two purchase orders as evidence. Here, however, the similarities end. Parties A and B, it turns out, are merchants and established trading partners engaged in a regular course of business involving the routine exchange of electronic purchase orders. The transaction at issue involved a standard commercial product and did not carry an extraordinary dollar value. Parties Y and Z, however, are strangers who, although they possess and utilize EDI capabilities, have never done business together before. Furthermore, the transaction was of a high dollar value and was for the purchase of a custom manufactured item.

Although the two EDI purchase orders were essentially identical, from an evidentiary standpoint the two transactions were totally different. The burden party A must carry in order to have its purchase order admitted into evidence is relatively light. The use of basic security techniques—password access control, generally reliable audit capability, probably the use of VAN—should suffice to have the evidence admitted. Party Y, however, must bear a heavier evidentiary burden. The controls used by party A might not suffice. Strong originator authentication, message integrity, and noM-repudiation—probably encryption techniques—would have been advisable.

Likewise, from the standpoint of the Computer Security Act’s risk-based standard, the two transactions bear little resemblance. For parties A and B, use of sophisticated and potentially costly security techniques as a supplement to routine control and audit practices would have been unnecessary to satisfy the Act. For parties Y and Z, they could have been essential.

In sum, the development of security plans as required by the Computer Security Act and good practice involves a common sense approach to risk assessment. Analyzing the security requirements of particular applications can be aided by considering the security characteristics which the application should possess as well as the sensitivity level for each. As enhanced security techniques become more cost effective and increasingly ubiquitous, the task will become easier. However, careful assessment of the tradeoffs must be made as part of this process. Attention to these factors should satisfy legal requirements.

RISK MANAGEMENT METHODOLOGY

It is important to manage risk, i.e., the likelihood of loss, as the basis for wise selection of security measures. If all systems were the same (i.e., the same size, transaction volume, information sensitivity, urgency, monetary activity level, and operating environment), it would be possible to define an appropriate security program and apply it to all EC systems without further consideration. This is not the case; EC systems vary in all the dimensions just mentioned. Consequently, it is not possible to define a single security program for all EC systems. EC risks can only be managed efficiently by using rational risk management. Perfect security (nothing will ever go wrong) is infinitely expensive and cannot be a rational design goal. On the other hand, inadequate security often leads to unnecessary losses.

RISK-SENSITIVE DESIGN

Risk cannot be managed abstractly. The first step in EC system development is to develop a basic system design that accomplishes the functional requirements of the EC system. However security features must be incorporated during the design phase. When the system design is sufficiently detailed, the risk management process can begin and specific data protection requirements identified. There are three parts to this process:

- Assessment of risks to determine what kinds and amounts of losses are likely to occur when the EC system becomes operational. Two loss categories are usually identified. (1) Losses caused by threats with reasonably predictable occurrence rates are sometimes referred to as "expected losses" and are expressed as average rates of loss in dollars per year. (2) If a threat has a very low rate of occurrence that is difficult to estimate, but the threat would cause a very high loss if it were to occur, the result would be referred to as a low-probability, high-consequence risk. This type of loss is often called a "single occurrence loss."
- Selection and implementation of security techniques that will reduce expected losses by an amount greater than the cost to implement the security techniques or reduce the fatal losses to tolerable levels.
- Periodic reexamination of risks after operational use begins to verify that security techniques continue to be effective, and to detect significant changes in the risk environment.

The initial risk assessment does not have to be highly detailed and precise. Instead, the objective should be to develop a broad understanding of inherent risks and potential security techniques to support the design effort. The first two steps are repeated as necessary during the design phase to refine the assessment; the selection of security techniques is optimized as the EC system design evolves.

Senior managers have a vital role in providing for a balanced development program for EC systems that includes adequate provision for security. Authorities agree that this role is essential to successful implementation of EC systems. Senior managers must ensure a proper balance is maintained between functionality and security during the design process.

ASSUMPTIONS

The assumptions used during this risk assessment are based on the Presidential memorandum and the ECAT charter. These specific assumptions include the following:

- The current paper-based procurement process will be automated during the business process improvement initiative to take advantage of security controls inherent in the EDI process.

- An EC approach for contracting and performing procurement functions can be implemented within 6 months, with additional capabilities planned for implementation within the 1- and 2-year time frames.
- Effective computer security programs are in place at Federal agencies to provide a baseline for implementation of security measures within the government EC initiatives.
- Risk control techniques that are expected to cost more than the risk occurrence may not be implemented. Other control techniques with more appropriate lower cost requirements can be adopted.
- EC for procurement functions involving classified data can be implemented when an appropriate level of protection is available.

CURRENT FEDERAL PROCUREMENT FOR SIMPLIFIED PURCHASES

The procurement process is initiated with a requirement generated from a business area. Procurement officials are required by the Federal Acquisition Regulation (FAR) to contact from one to three potential suppliers before award is made. Contact of potential suppliers is accomplished by telephone, fax, or E-mail, and a vendor is chosen. For simplified purchases (below $25,000), the procurement process is paper based after a vendor is selected to provide the required product.

A requisition is forwarded to the budget office for funding and sent to procurement for preparation of a purchase order. The paper-based system process continues when the purchase order is forwarded to budget, accounting, and the selected vendor. Upon receipt, the vendor processes the order, ships the goods, and sends an invoice to agency accounting. Here the invoice is held, pending receipt of a receipt report from the ordering organization. When the report is received, accounting matches the invoice, purchase order, and receipt report; prepares disbursement transaction for payment; and releases payment on due date.

RISKS

The process above provides us with some insight on risks associated with the current procurement process for simplified purchases. Several factors substantiate the conclusion that risks are extremely low:

- Trading partners are known to procurement officials through previous business exchanges (specific telephone numbers used, voice recognition, vendor performance).
- Methods used to communicate business requirements are of a protected nature (telephone, fax, and trusted mail service provided by the U.S. Postal Service or other trusted third parties).
- The paper-based system process (requisition, purchase order, invoice, receipt report, and payment) is subjected to extensive administrative controls at each stage of the acquisition process, which provide adequate protection against threats associated with modification, loss, and repudiation. Inefficient as they may be, traditional paper-based communications satisfy basic security requirements described below.

SECURITY REQUIREMENTS

There are four requirements for the security of any process including the simplified purchase procedures:

- Confidentiality—ability to limit access to the information contained in a communication. This has generally been accomplished with some combination of security markings, envelopes, and trusted messengers (U.S. Postal Service, Federal Express, etc.).
- Message integrity—assurance that the content of a communication is complete and has not been changed prior to receipt. This is accomplished by a number of features, the primary ones being those associated with the use of writing itself: inks that make erasure and alteration easily perceptible, salutations and closings that constrain the length of the message, and the size of the paper (form) that may limit the addition of text.
- Originator authentication—assurance that the communication originated with the named source. This is most commonly provided by the handwritten signature. The authentication purpose of the signature has two conceptual parts. First, it adds

a degree of formality, increasing the likelihood of actual assent to the terms contained in the document. Second, it serves to identify the document with the originator, because signatures tend to be unique. In the simplified purchase process, these functions are served primarily by the use of pre-printed forms.

- Nonrepudiation— stronger form of authentication that relates to the ability of a disinterested third party to reasonably conclude that the identified originator intended to be bound by the substance of the communication. Specifically, the originator cannot deny he sent the message and the receiver cannot deny he received it.

FEDERAL PROCUREMENT THROUGH ELECTRONIC COMMERCE

The use of electronic commerce techniques does not necessarily increase transactional risk beyond that experienced in a paper-based environment. This is in spite of the fact that, unlike paper-based communications, electronic communications theoretically can be changed without a trace. However, relevant communications protocols such as X.400 and the evolving X12.42 and X12.58 standards themselves contain headers, password fields, and control information relevant to data protection mechanisms. These data protection characteristics, coupled with the speed of communication afforded by EDI, decreases the likelihood of successful interception of specific transaction sets. Deliberate modification implies that specific transaction sets are being targeted. In most cases, it would be quite difficult technically to locate a specific transaction set, intercept it, modify it, and then insert it back into the data stream without causing an error condition or otherwise having the modification activity detected. Viewed from the standpoint of potential threats, controls should make the cost of obtaining data greater than the potential value of obtaining or modifying the data. This is especially true within the simplified purchase process where the majority of procurement transactions (98 percent) within the Federal government fall below the $25,000 threshold. However, a small purchase order could have totals changed to fix small problem amounts if no check is performed. Controls available for data protection will be discussed below.

NEW METHODS/NEW RISKS

Implementation of an EC system requires more care than a traditional automated business system because of four factors unique to EC:

- Most traditional paper records are eliminated. The electronic documents that replace paper documents are extremely important. Care must be taken to safeguard them against loss and alteration and to ensure that any document can always be retrieved from the secure data base in which it has been stored.
- Human participation in routine transaction processing is limited or nonexistent. Human oversight in paper-based systems has provided formal and informal reasonableness testing and error detection and correction. The EC application programs and the EDI software must include comprehensive controls and checks to replace all aspects of routine human oversight while providing detection of exceptional conditions that trigger special human intervention. This report does not attempt to make a sharp distinction between "security procedures and techniques" and "internal controls and checks." Both security and control objectives are commonly served by the same measures.
- Transactions are processed more rapidly, leaving less time to detect and correct errors. Errors must be detected and corrected quickly, before automatic initiation of subsequent actions that will be expensive to correct.
- The computer systems of trading partners (government and commercial) communicate directly with one another. Each trading partner depends on the accurate and timely performance of the other partners and the EC integration components, to include the data communications network that connects them. EC commonly leads to reengineering of business systems to take advantage of the speed and efficiency inherent in EC. As a result, each trading partner must be prepared to recover quickly from system failures to avoid having an impact on operations of the other trading partners. Interrupted transactions must not be lost or incorrectly duplicated as a result of retransmission.

RISK ASSESSMENT

Risk analysis, or assessment, is accomplished to determine both the impact and potential frequency of occurrences. The calculation of risk is based on the estimated frequency or probability of a threat occurring and the order of magnitude estimated loss per occurrence. A formula for calculating risk is in Federal Information Processing Standard Publication No. 65 (FIPS PUB 65). This formula combines frequency of threat occurrence with damage impact to produce an annual loss expectancy (ALE). For the purpose of this analysis, the probability of risk occurrence and impact are based on expert judgment, not empirical data.

RISK ASSESSMENT PROCESS

Risk assessment will be treated as a subset of risk management and shall be defined to mean "the process to determine a measurable expectancy of loss, expressed in terms of frequency over a given unit of time, and the amount of potential loss to the identified assets." This section is divided into three areas: risk identification, risk analysis, and prioritization.

The key result of this assessment process is the development of a rough order of magnitude estimate of risk. The calculation is based upon the estimated frequency, or probability, of a threat occurring and the estimated loss per occurrence. To estimate frequency, we considered the threat source and the motive or cause. To estimate the loss, we used expert judgment to consider the estimated asset value and the extent of damage that would potentially result from a threat occurrence.

The formula used for the calculation was taken from FIPS PUB 65. This formula combines frequency of threat occurrence, given as "P," with damage impact, given as "D," to produce an annual dollar loss, given as ALE. Given that these estimates will be imprecise, this formula uses order-of-magnitude scales for both frequency and damage:

P = Rating for the frequency of occurrence for a threat

0	Virtually impossible
1	Once in 300 years
2	Once in 30 years
3	Once in 3 years (1,000 working days)
4	Once in 3 months (100 working days)
5	Once in 10 days
6	Once each day
7	Once every 2 hours (10 times per day)
8	Once every 15 minutes (100 times per day)

D = Rating for the amount of damage caused

0	Less than $1
1	$10
2	$100
3	$1K
4	$10K
5	$100K
6	$1M
7	$10M
8	$100M

These "P" and "D" ratings are substituted into the following equation to compute the ALE:

ANNUAL LOSS EXPECTANCY = $10^{(p+d)}$/ $3k per year

To simplify manual calculations, the following values were used. (The ALE values are approximate; however, they are still reasonable given the imprecision of the inputs.)

P + D =	6	7	8	9	10	11	12
ALE =	300	3K	30K	300K	3M	30M	300M

EXAMPLE: The contents of a computer room have been valued at $10 million. Should a flood occur, the expected damage is estimated at approximately $100,000. The frequency of flooding is estimated to be once in 30 years based on the existence of few threat sources and reasonably effective safeguards. Given the previous scales, the ratings D = 5 and P = 2 can be assigned. Applying these values to the table yields ALE.

RESULTS OF THE ECAT RISK ASSESSMENT

Each risk identified is first described, the nature is then stated, and an impact analysis is provided in terms of both tangible and intangible impact. An overall approach to manage and minimize the risk and a specific approach or tactic is then described; rank order of importance is not delineated. This section addresses those specific risks associated with implementation of EC in contracting.

DATA DESTRUCTION

Hardware, software, and data must be protected from direct or inadvertent tampering. Because EDI requires electronic connectivity with a large number of networks and processors outside agency control, the system is vulnerable to unauthorized access. Unauthorized access can come in many forms (e.g., virus, illegal entry) and can cause significant damage, violate the confidentiality of vital information, and impede competition. Even those under agency control will be more vulnerable to inadvertent security violations due to data sharing and distributed processing.

Impact Analysis

Damage to software or data can cause loss of time and increase expense to support procurement systems.

- Tangible Impact
  - Costly processing time correcting damaged system software or data base reconstruction may result.
  - Delays in the procurement process will prove costly due to loss of data necessary to complete the procurement process , as well as initiate payment for goods and services.
- Intangible Impact
  - Loss of public confidence in the procurement process.

Management Plan and Approach

Avoiding and minimizing security risks are the goals. System software protection through efficient configuration management and access controls should be implemented.

Access controls are in place at agency standard systems through use of login identification and passwords for authorized system users. Passwords are user generated and changed at least monthly through computer generated prompts. Use of this process establishes a list of authorized system users with additional authorization to generate contracting EDI transactions.

Many of the value-added networks have similar access controls in place for authentication of trading partners as authorized users of the VAN services. Procedures for the VAN follow closely those of the government in that passwords must be a minimum of eight alphanumeric characters, be user generated, and be changed monthly.

Virus protection software products are essential to avoid denial of service and are available commercial off-the-shelf (COTS).

UNAUTHORIZED ACCESS TO CONTRACTOR QUOTE DATA

Access to contractor quote data is limited to only those procurement officials involved in the procurement. Every reasonable effort is made to ensure that quote data is protected from disclosure. Any communication method used to transmit procurement data must protect the confidentiality of the data. EDI procedures and communications architectures must maintain the level of security implemented by the trading partner.

Impact Analysis

Unauthorized access to vendor responses to request for quotes may disclose proprietary business information which would adversely impact vendor participation in future bids for requests for goods or services.

- Tangible Impact
    - Legal action may result if quote data were inappropriately disclosed. However, since the average small purchase is

valued at $1,250, we anticipate the damage is minimal.

- Intangible Impact
  - Loss of public confidence could result if quote information is disclosed to unauthorized individuals.

Management Plan and Approach

Confidentiality can be ensured only through encryption of the transaction implemented by the trading partner until it is received by the destination application system and opened by the message recipient. This method provides true end-to-end protection of the sensitive business data transaction.

DATA INTEGRITY

Overall security responsibility belongs to the owner of the business process. The contracting activity must be assured that the data transmitted is received in total by the trading partner.

Impact Analysis

Failure to receive a complete transaction set, or loss or modification of a transaction set will have both tangible and intangible impacts on the contracting process.

- Tangible Impact
  - Costs incurred as a result of nonavailability of the product or service.
  - Loss of administrative lead time.
  - Increased procurement lead time.
- Intangible Impact
  - Loss of public confidence in the ability to conduct business via electronic commerce.
  - Adverse impact on vendor community.

Management Plan and Approach

A technique that helps assure message integrity is the implementation of hash totals in the EDI transaction. A hash total is a summation for checking purposes of similar fields in a file, such as fields containing part numbers or national stock numbers, that would otherwise not be summed. Once the transaction is received, the data are regenerated and compared for equality. In the event the data do not compare, the data are rejected by the receiving activity. The DSA does not provide an inverse function. Hence, the message is not encrypted; only the hash total is encrypted. Therefore, DSA provides authentication but no confidentiality.

ELECTRONIC SIGNATURES

Documents are executed with electronic data codes, encrypted or otherwise protected, which signify approval by the named official. Many contractors and Government offices are reluctant to accept electronic documents due to the absence of a signature or other electronic means of identifying the sender of the transaction.

Impact Analysis

Losses from this risk are both tangible and intangible.

- Tangible Impact
  - Costs to the organization due to continued manual and limited automated support for labor intensive tasks.
  - Costs to the organization through potentially higher prices for procured supplies and services processed manually.
  - Costs incurred as a result of potential nonavailability of the supply item or service in a timely manner.
- Intangible Impact
  - Loss of industry confidence and support to the Federal EC program.

Management Plan and Approach

A digital signature provides additional security and enables a message recipient to verify the originator of the message as well as the message content. A Digital Signature Algorithm (DSA) which uses the Secure Hash Algorithm is currently being considered for adoption as a FIPS PUB. The DSA does not provide an inverse function. Hence, the message is not encrypted; only the hash total is encrypted. Therefore, DSA provides authentication but not confidentiality.

The DSA employs two cryptographic keys for each user. Each user has a public key that is known by all potential trading partners and a private key that is kept secret. The message to be sent serves as input to the SHA; the output of the SHA operation is the message digest. The message digest and sender’s private key are used in a signing algorithm to calculate the digital signature. The recipient receives both the message and digital signature.

A signature verification algorithm is used by the message recipient to authenticate the signer of the transaction. This algorithm uses input from the sender’s public key, the received digital signature, and message digest recalculated with the SHA from the received transaction. If the recalculated component matches the component as received, the signer is authenticated and the received message is identical to that sent. If the signature fails to verify, the transaction is rejected and retransmission requested.

Implementation of the public key technique described above requires implementation of a high-security public key infrastructure. This system would provide secure distribution of private keys, and a trustworthy source of public key information. As we migrate from simplified purchases to procurements of high dollar value and request for proposals under the contracting business area, the need for a public key technique for data protection will become apparent.

AVAILABILITY (CONTINUITY OF OPERATIONS)

EC capability will be implemented on COTS computer hardware and software. Information will reside at many sites and be transported over agency networks to/from industry systems/networks. Service interruption is the inability to transmit data from the procurement automated information system to the gateway and from the VAN user to agency systems.

Business activities supported by EDI will become dependent upon information technologies. Catastrophic failures could bring the associated business activities to a halt. Service interruption impairs the ability of the contracting activity to conduct business via EC.

Impact Analysis

The reliability of hardware/software will have tangible and intangible impact on the availability of contracting information. This may include the ability to make an award, thus delaying transaction processing.

- Tangible Impact
    - Nonavailability of systems can be costly to contracting offices.
    - Lack of accessibility to data can cause financial loss to an organization.
    - Costs incurred as a result of nonavailability of the product or service during a system outage.
    - Delays realized in identifying alternate means of acquiring product or service during system outage or litigation process.
    - Contractor loss of revenues.
- Intangible Impact
    - Loss of prestige to the organization or automated process providing the service.
    - Loss of public confidence.

Management Plan and Approach

Many different technical and programmatic techniques will reduce the chances of a catastrophic loss of continuity. There are many ways of providing capabilities, each with increased costs. One VAN, automated information system (AIS), or gateway could be cross-connected to provide alternative connectivity. This would require the sizing of those cross-connected networks to assume the workload of the other. Detailed test plans must be developed and used to ensure compatibility, accuracy and availability of the cutover systems.

Highly reliable COTS hardware and software ensure sustainability. Several technical capabilities are available at an incremental cost. Redundant systems for cutover, as an example, may be cost prohibitive. Federal agencies should ensure continuity of EC processes is addressed in agency ADP Continuity of Operations Plans.

Table M-1 summarizes the functional and technical risks. This table also provides a summary of the risk estimate computed and groups the risk estimates into low, medium, or high categories.

Table M-1. Risk Assessment Summary

			ANNUAL LOSS ESTIMATE (D + P)						
			LOW		MEDIUM			HIGH	
RISK	**IMPACT RATING (D)**	**FREQ. RATING (P)**	**$300 OR LESS 6**	**$3K 7**	**$30K 8**	**$300K 9**	**$3M 10**	**$30M 11**	**$300 M 12**
UNAUTHORIZED ACCESS TO CONTRACTOR QUOTE DATA	**3**	**2**	**X**						
DATA INTEGRITY	**5**	**4**				**X**			
DATA DESTRUCTION	**2**	**8**					**X**		
ELECTRONIC SIGNATURES	**3**	**3**	**X**						
AVAILABILITY	**6**	**4**					**X**		

SECURITY REQUIREMENTS

The impact is being addressed based on tangible and intangible valuation qualities as depicted in Table M-2 below.

Table M-2. Tangible-Intangible Evaluation

VALUATION QUALITY	THREAT IMPACT
Replacement	Destruction
Confidentiality	Disclosure
Integrity	Modification
Availability	Delay or Denial
Proof of Origin	Repudiation

An example of each of these five valuation qualities and corresponding threat impacts is provided below:

- The cost of replacement of quote data because of its destruction is being evaluated based on the cost of delayed awards as well as the inability to use the system if this loss is frequent.
- The loss of confidentiality as a result of the inappropriate disclosure of quote information results in the compromise of proprietary business data, as well as the potential for costs of legal action should litigation result.
- A loss of integrity is based on the impact of modification of contract quantities or requirements.

- Availability includes both the cost to government and industry when the EC capability is inappropriately denied and not available for immediate use.
- Proof of origin and receipt of X12 EDI transactions are required to support nonrepudiation.

The ALE is determined based on the estimated frequency of occurrence multiplied by the impact. A prioritized list of all identified and analyzed risk items has been completed in order to focus on development of a plan to control risk.

As the Federal government moves to implement EC within the contracting business area, consideration should be given to the effect of EC technology on the effectiveness of traditional controls previously described in the paper-based procurement process. The transition to an EC environment will transform business processes from paper-based to EDI transaction sets. These standard business transactions have many of the same security requirements as the forms they replace. However, implementation of these data security requirements within computer processes pose unique solutions which must be tailored to the particular transaction.

Table M-3 lists each of the standard ANSI X12 transactions identified for use with the EC in contracting business process improvement initiative and provides the security objectives of each based on protection requirements.

It is important to recognize that, for simplified purchases, it is the substance of the transaction and what it represents to the business community that requires protection, rather than its data contents. Established protection requirements are consistent with guidance set forth in the Computer Security Act of 1987.

Table M-3. Rationale for Security Objectives for Each Transaction Set

Transaction Set/ Security Objective	Confidentiality (Data disclosure)	Integrity (Modification)	NoM-Repudiation (Proof of Origin & Receipt)	Auditing (Retention of Audit trail)
840: Request for Quotation		Ensure accuracy, avoid modification of RFQ		Record transaction passing through the EC System
843: Response to Request for Quotation	Nondisclosure required to protect proprietary information (optional)	Ensure accuracy, avoid modification of 843		Record transaction passing through the EC System
850: Purchase Order		Ensure accuracy of quantities and purchase price	Proof of receipt critical, proof of origin necessary for internal auditors	Record transaction passing through the EC System
824: Application Advice				Record transaction passing through the EC System
836: Contract Award Notice				Record transaction passing through the EC System
838: Trading Partner Profile	Nondisclosure required to protect proprietary information (e.g., vendor performance)	Ensure accuracy, avoid modification of vendor registration		Record transaction passing through the EC System
864: Text Message	Nondisclosure required to protect proprietary information (optional)	Ensure accuracy to protect general info.	Proof of receipt critical, proof of original necessary for internal auditors or to ensure messages reach the appropriate individuals	Record transaction passing through the EC System
997: Functional Acknowledgment			Proof of receipt critical, proof of origin necessary for internal auditors or to ensure messages reach the appropriate individuals	Record transaction passing through the EC System
832: Prices/Sales Cat.		Ensure prices are accurate from Trading Partner		
855: Purchase Order Acknowledgment		Ensure accuracy of the order purchased	Proof of origin & receipt for legal reasons (IAW procurement guidelines)	Record transaction passing through the EC System
860: Purchase Order Change Request-Buyer Initiated		Ensure accuracy of the order purchased	Proof of origin & receipt for legal reasons (IAW procurement guidelines)	Record transaction passing through the EC System
865: P.O. Change Ack. Request Seller		Ensure accuracy of the order purchased	Proof of origin & receipt for legal reasons (IAW procurement guidelines)	Record transaction passing through the EC System
869: Order Status Inquiry				Record for legal reasons, need to know if inquiries were made (EC System)
870: Order Status Report				Record for legal reasons, need to know if inquiries were made (EC System)
810: Invoice		Ensure accuracy of the invoice	Proof of origin & receipt for legal reasons (IAW procurement guidelines)	Track invoice: Record for legal reasons (EC System)
841: Spec/Tech Info	Nondisclosure required to protect proprietary information	Ensure accuracy of technical documentation	Proof of origin: correct source of tech info.; proof of receipt: ensures Gov't received tech info.	Track tech info.: Record for legal reasons (EC System)
842: NoM-Conformance Report	Nondisclosure required to protect info. that may be damaging to trading partner	Ensure accuracy of report	Proof of origin & receipt for legal reasons (IAW procurement guidelines)	Record for legal reasons (EC System)
856: Ship Notice/Manifest	The location where the product is being shipped may be sensitive	Ensure accuracy of ship notice/manifest	Proof of origin & receipt for legal reasons (IAW procurement guidelines)	Record for legal reasons (EC System)

SECURITY TECHNIQUES

Risk management refers to the activities associated with actions taken following a risk assessment. After the risk assessment is completed, countermeasures may be identified and deployed to eliminate those risks or reduce them to an acceptable level. Available solutions identified by the ECAT are provided below:

- Confidentiality refers to the need to restrict sensitive information from being disclosed to unauthorized recipients. Available solutions include
  - access controls (login ID, passwords, smart cards, key locks, physical access) and
  - data encryption (data encryption standards).
- Message integrity is provided by ensuring that messages are changed only in a specified and authorized manner, as follows:
  - Imbedded references—including a unique identification code with each transaction to distinguish it from all others.
  - Message repetition acknowledgment—sending an acknowledgment that repeats messages or parts of messages.
  - Internal message verification—recalculating and verification of message character totals (hash totals) for checking similar fields.
  - Cryptographic techniques—using message authentication codes (MAC), digital signatures, and public key encryption.
- Authentication is assurance to a message recipient that the source of the message is the named originator or the intended recipient. Originator/recipient authentication can be provided by
  - Imbedded references (EDI sender/receiver codes), which are numbers or passwords both parties have agreed to use;
  - TPA, which requires each activity to submit a discrete authentication code within a specified segment of the transaction set;
  - Functional acknowledgment (e.g., an ANSI X12 997 transaction set), which can be dispatched to notify the originator that a transmission has been received and either accepted or rejected; or

  - Trusted third party (i.e., an EDI VAN), which can provide additional originator authentication since only authorized users can access the EDI VAN to retrieve or deposit EDI transactions from or to a particular EDI mailbox.

- Nonrepudiation provides assurance that one of the two parties to a data interchange cannot falsely deny involvement due to proof that can be offered to a third party. In addition to the techniques listed above for authentication, the following techniques provide strong protection against nonrepudiation:

  - Third-party notarization (EDI VAN)
  - Electronic signatures
  - Audit trails that provide history files of transactions generated with identification of the sender or receiver.

- System availability ensure continuity and includes data backup and recovery procedures. Archived data are often used for backup and recovery purposes. Virus protection software (COTS software) will provide protection from the introduction of viruses resulting in a loss of system availability.

DEVELOPMENT OF A RISK MANAGEMENT PLAN

The key step in controlling risk is the development of a risk management plan that addresses each of the risk items, how they interrelate, and how they are related to the overall project. The ECAT has reviewed three methods for risk management:

- Risk avoidance. Risks can be avoided through detailed security planning during the design and implementation of EC capability. Effective security planning requires the coordinated efforts of representatives from the business area, security, and technical disciplines.

- Risk control. This practice involves establishing a mechanism for eliminating or reducing the effects of occurrence. One of the mechanisms used in risk control is the development of a resolution approach with specified actions and milestones.

- Risk acceptance. The conscious decision on the part of senior management to accept a risk due to the low threat of occurrence or cost prohibitive security countermeasures.

RISK CONTROL PLAN

An appropriate resolution of identified risks is to map the specific functional and technical risks to the appropriate security technique. The security officer of the organization responsible for an application must evaluate and make recommendations to ensure that an appropriate level of security is provided.

MONITORING

In order to ensure the effectiveness of the controls initiated in the risk management plan, risk monitoring will be accomplished by the responsible organization. Each of the risk handling techniques will be assessed during implementation to assure implementation has the planned effect on reducing or eliminating risks as described above.

Implementation of mechanisms to eliminate or reduce identified risks will be monitored throughout the 6-month, 1-year, and 2-year development periods for the EC effort. During these periods, the success of risk handling techniques will be evaluated and if necessary more stringent control initiated. Revision and update of this risk management plan will be accomplished as necessary.